REMARKS

Claims 1-13, 15-27, and 30-38 are active in the application. Claims 14, 28, and 29 have been cancelled. Claims 36 and 37 have been added to the application and incorporate the language suggested by the Examiner in the Office Action. Claim 38 has been added to the application, and is supported by the specification in paragraph 34 where it is stated that the clock runs at a high speed so that hundreds of thousands or millions of clock cycles occur.

Applicant notes with appreciation that claims 30 and 31 have been allowed, and that claims 1-29 and 34-35 have been identified as being potentially allowable.

Claims 1-29 and 34-35 were rejected under 35 USC 112, second paragraph as being indefinite. Specifically, the word 'unpredictable' was objected to as being "open to various interpretations".

In the present invention, the unpredictable number of cycles is determined by a human action of unpredictable duration. The duration of the human action determines the duration that the clock drives the counter. This limitation has been added to claims 1 and 21. As described in the present specification (see paragraph 0034), the clock can be operated for the duration of time it takes for the user to enter the PIN, the duration of time between PIN entry and data communication with the card reader, or the length of time a user holds down a button. All these exemplary methods depend upon human actions to start or stop the clock. Such human actions have inherently unpredictable timing on the time scale relevant to the high speed clock, and hence can be relied upon to generate an unpredictable number of clock cycles. Thus, in the present application, "unpredictable" refers to the unpredictable number of cycles of a clock that is started or stopped at a time determined by a human action. This explanation, plus the amendment to claims 1 and 21, and the addition of dependent claims 36 and 37 which are fully enabled by the specification should now make clear the metes and bounds of the claimed invention. Therefore, withdrawal of the rejection under 35 U.S.C. 112, second paragraph, and allowance of claims 1-13, 16-27, and 34-37 is requested.

Claims 32 and 33 were rejected under 35 USC 103(a) as being unpatentable over US patent 5,478,994 to Rahman et al. This rejection is traversed.

A basic difference between Rahman and the claimed invention is that Rahman's invention deals with stored pseudo random numbers, while the claimed invention deals with pseudo random numbers that are generated for each transaction. The comparison with the pseudo random numbers at the server is done with stored numbers for Rahman, while, in contrast, in the claimed invention, it is done with numbers that are generated for each transaction. This is captured in Claim 32 where it is required that: "authenticating the credit card by comparing the outputs produced in step (b) with settings of the counter and GEN known to the financial institution". Rahman et al. do not teach or suggest transmitting the counter output to the host computer.

In view of this, claims 32 and 33 should be allowable over the Rahman reference.

With respect to claim 37, Rahman does not show or suggest involvement of a human action that is determined by one of a duration a keypad is pressed, a duration between two keypad entries, or a duration between card activation and communication with a card reader.

Claim 38 requires that the counter and GEN are each driven for a plurality of cycles. In contrast, Rahman et al. teach a credit card that stores a series of random numbers. The random numbers are stored in a programmable memory (PROM). Each time the card is used in a financial transaction, one of the random numbers is used for authentication. A counter 26 records the number of transactions over the life of the card.

As noted in the Office Action, the counter and PROM of Rahman et al. are each incremented exactly <u>once</u> per transaction. The counter of Rahman et al. cannot reasonably be altered to increment more than once per transaction because *the counter of Rahman et al. is used to count the number of transactions* (see col. 3, lines 19-23). By comparison, the counter of the present claim 32 *counts the number of cycles experienced by the GEN in a single transaction.* The fixed or predictable mathematical relationship between the counter and GEN of the present invention is required so that the number of cycles experienced by the GEN is counted. The present counter does not count the number of transactions. Hence, the present counter is very different from the counter of Rahman et al. Additionally, the PROM of Rahman et al. is incremented exactly once per transaction. With each transaction, the PROM provides the next number of the random number sequence. There exists no teaching or motivation to increment the PROM more

than once per transaction and thereby skip numbers stored in the PROM. By comparison, the GEN of the present invention is cycled thousands or millions of times for each transaction, so that a random number is generated.

Also, Rahman et al. requires that only the random number from the PROM be sent to the host computer for authentication. The host computer of Rahman et al. does not use the output of the counter 26 (see col. 3, lines 25-27 and 29-36). This is because the host computer maintains a record of the number of transactions (see col. 3, lines 51-53), and the sequence of random numbers received by the host computer. The host computer of Rahman et al. is able to authenticate with only the random number from the PROM. In Rahman et al., *only the random number from the PROM is required for authentication.* By comparison, in the present invention, *both the counter output and GEN output are required for authentication.* Additionally, since Rahman et al. employ a stored series of random numbers, the PROM of Rahman et al. generates a random number that is predictable from the number used in the prior transaction (assuming the PROM data is known). The present GEN, by comparison, produces numbers that are not predictable from the numbers used in the prior transaction. This is because the output of the GEN is determined by the number of cycles experienced by the GEN, and the number of cycles is different for each transaction.

In view of the foregoing, it is respectfully requested that claims 1-13, 15-27 and 30-38 be allowed.

Should the Examiner find the application to be other than in condition for allowance, the Examiner is requested to contact the undersigned at the local telephone number listed below to discuss any other changes deemed necessary in a telephonic or personal interview.

A provisional petition is hereby made for any extension of time necessary for the continued pendency during the life of this application. Please charge any fees for such provisional petition and any deficiencies in fees and credit any overpayment of fees for the petition or for entry of this amendment to International Business Machine's Deposit

5   Account No. 09-0458.

Respectfully submitted,

Michael E. Whitham
Reg. No. 32,635

10

Whitham, Curtis, & Christofferson, P.C.
11491 Sunset Hills Road, Suite 340
Reston, VA, 20190

15

Phone: 703-787-9400
Fax: 703-787-7557

Customer Number 30743

20

10/709,112   (00750490AA)